UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/810,500	03/26/2004	Masakazu Nishida	9683/175	8158

7590 12/09/2008

Brinks Hofer Gilson & Lione
NBC Tower
Suite 3600
P.O. Box 10395
Chicago, IL 60610

EXAMINER	
ROSE, KERRI M	

ART UNIT	PAPER NUMBER
2416	

MAIL DATE	DELIVERY MODE
12/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/810,500	NISHIDA ET AL.	
	Examiner	Art Unit	
	KERRI M. ROSE	2416	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 August 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *6-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *6-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Please note AU 2616 is now AU 2416.

2. Applicant's arguments with respect to claims 1-5 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 6-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind et al. (US 6,826,690) in view of Imamura et al. (US 6,453,369).

In regards to claim 6, Hind discloses a computer terminal (figure 1a illustrates a workstation) comprising: a processor (fig. 1a.12) in communication with (fig. 1a.14 is a bus for communication) a memory (fig. 1a. 28 and 30) and a receiver (fig. 1a.32 is a network communications line); the receiver configured to communicate over a network wherein the receiver is further configured to receive a first program from a first server (Col. 7 line 34 indicates the workstation may be in a client/server relationship. Col. 9 line 37 indicates the described security method may be applied to any message exchange. Downloading a program is a type of message exchange.);

the processor configured to store in the memory the first program and a first communication address of the first server from which the first program is downloaded (Col. 9

line 23 indicates a globally unique device identifier, which may be considered an address, is stored in the memory shown in fig. 1b.35. When information, such as a program download, is exchanged, it must be stored in memory, such as that shown in fig. 1a.28.);

wherein the memory is further configure to store a second program and a second address of a second server from which the second program was downloaded and data associated with the second program (Col. 9 line 37 indicates the security method is performed with any and all message exchanges. This implies there are multiple communications between the client and server, any two of which can be program downloads. Every program download will be handled the same way, i.e. the program and address information are stored in memory.).

Hind discloses matching the device identifiers to establish the identity of the program originator in col. 9 lines 57-65.

However, Hind is silent to the processor further configured to execute the first program stored in the memory; in response to a request from the first program executed on the processor to access the data associated with the second program, the process further configured to determine whether the first communication address matches the second communication address; and the processor further configured to permit the first program to access the data associated with the second program based upon the determination that the first communication address of the first server matches the second communication address of the second server.

Imamura discloses running a first program in steps 401-403 of figure 10. In step 406 the identifiers are checked to determine if the first and second addresses match. Steps 407-415 illustrate the different read/write enable/disable combinations possible depending upon the type of identifier match(es) found by Imamura.

It would have been obvious to one of ordinary skill in the art at the time of the invention to use the security matching taught by Imamura in the authentication method of Hind because doing so helps ensure secrecy and security of data, as disclosed by Imamura in column 1 lines 46-48.

In regards to claim 7, Hind and Imamura disclose the computer terminal of claim 6 further comprising: a user interface in communication with the processor, the user interface configured to receiver a suer input from a user of the computer terminal (Hind fig. 1a.18-22 disclose interface and input devices. Imamura fig. 1.3 and 4 disclose interface and input devices.);

the processor further configured to generate with the user interface a request for permission for the first program to access the data associated with the second program (Imamura fig. 16.s910 disclose entering a password for user permission.);

the processor is further configured to receive the user input from the user interface and determine whether the first program has permission to access the data associated with the second program based upon the user input (Fig. 16.s907-910 discloses determining permission based in part upon the input password.);

wherein the processor is configured to determine whether the first communication address of the first server matches the second communication address of the second server in response to determination that the user input indicates permission for the first program to access the data associated with the second program (fig. 16.s907 discloses checking that the addresses match provided that the password is correctly input.).

In regards to claim 8, Hind and Imamura disclose the terminal of claim 6 further comprising: the processor further configured to determine whether the second program permits another program to access the data associated with the second program (Imamura fig. 10 discloses different read/write enable/disable combinations. The second program may permit complete, partial, or no access to its data.);

and in response to determination that the second program permits another program to access the data associated with the second program the processor configured to permit the first program to access the data associated with the second program based upon the determination that the first and second addresses match (fig. 10.s406 discloses checking the addresses for a match.).

In regards to claim 9, Hind and Imamura disclose the terminal of claim 8 wherein in response to determination that the second program prohibits another program to access the data, the processor configured to generate with the user interface an indication that the second program prohibits the first program to access the data (Hind discloses displaying a reject message when the programs cannot interact in fig. 8a.855.).

In regards to claim 10, Hind and Imamura disclose the terminal of claim 8 further comprising: a user interface in communication with the processor wherein the user interface is configured to receive permission for the first program to access the data associated with the second program (Imamura figs. 6a and b disclose setting security level information. The stored information is used in the future to determine permissions relating to access for the first and second program. Hind discloses storing device certificates and private keys for future determinations in fig. 4.).

In regards to claim 11, Hind and Imamura disclose the terminal of claim 10 further comprising: the processor further configured to store registration information for the first program and the second program based upon the received permission and permit access in the future based upon the stored information (Imamura figs. 6a and b disclose setting security level information. The stored information is used in the future to determine permissions relating to access for the first and second program. Hind discloses storing device certificates and private keys for future determinations in fig. 4.).

In regards to claim 12, Hind and Imamura disclose the terminal of claim 6 wherein the first and second communication addresses are uniform resource locator (Hind discloses a client/server relationship in which the client may communicate over an IP network, such as the internet in col. 8 line 65—col. 9 line 20, among the network options. Such a setup requires the use of URLs.).

In regards to claim 13, Hind and Imamura disclose the terminal of claim 6 wherein the first program is associated with a first portion of the memory (Inherent; When a program is stored into memory a certain "block" of memory is allocated for its use.); the second program is associated with a second portion of the memory and wherein the data of the second program resides in the second portion (Inherent; When a program is stored into memory a certain "block" of memory is allocated for its use, including storage of data related to the program.);

and wherein the processor is further configured to access the second portion to permit the first program to access the data associated with the second program based upon determination that the first and second addresses match (Hind discloses matching the device identifiers to establish the identity of the program originator in col. 9 lines 57-65. Imamura discloses running

a first program in steps 401-403 of figure 10. In step 406 the identifiers are checked to determine if the first and second addresses match. Once the match is established the only way to grant access to the second data is for the processor to access the second portion of memory.).

In regards to claim 14, Hind discloses a method executed on a mobile computer terminal (figure 1a illustrates a workstation. Col. 8 lines 53 and 54 disclose the workstation may be mobile) comprising: a processor (fig. 1a.12) in communication with (fig. 1a.14 is a bus for communication) a memory (fig. 1a. 28 and 30) and a receiver (fig. 1a.32 is a network communications line); the receiver configured to communicate over a network wherein the receiver is further configured to receive a first program from a first server (Col. 7 line 34 indicates the workstation may be in a client/server relationship. Col. 9 line 37 indicates the described security method may be applied to any message exchange. Downloading a program is a type of message exchange.);

the processor configured to store in the memory the first program and a first communication address of the first server from which the first program is downloaded (Col. 9 line 23 indicates a globally unique device identifier, which may be considered an address, is stored in the memory shown in fig. 1b.35. When information, such as a program download, is exchanged it must be stored in memory, such as that shown in fig. 1a.28.);

wherein the memory is further configure to store a second program and a second address of a second server from which the second program was downloaded and data associated with the second program (Col. 9 line 37 indicates the security method is performed with any and all message exchanges. This implies there are multiple communications between the client and server, any two of which can be program downloads. Every program download will be handled

the same way, i.e. the program and address information are stored in memory.). Hind discloses matching the device identifiers to establish the identity of the program originator in col. 9 lines 57-65.

However, Hind is silent to the processor further configured to execute the first program stored in the memory; in response to a request from the first program executed on the processor to access the data associated with the second program, the process further configured to determine whether the first communication address matches the second communication address; and the processor further configured to permit the first program to access the data associated with the second program based upon the determination that the first communication address of the first server matches the second communication address of the second server.

Imamura discloses running a first program in steps 401-403 of figure 10. In step 406 the identifiers are checked to determine if the first and second addresses match. Steps 407-415 illustrate the different read/write enable/disable combinations possible depending upon the type of identifier match(es) found by Imamura.

It would have been obvious to one of ordinary skill in the art at the time of the invention to use the security matching taught by Imamura in the authentication method of Hind because doing so helps ensure secrecy and security of data, as disclosed by Imamura in column 1 lines 46-48.

In regards to claim 15, Hind and Imamura disclose wherein the first provider identifier includes a first network address and the second provider identifier includes a second network address (Hind col. 9 line 23 indicates a globally unique device identifier, which may be considered an address, is stored in the memory shown in fig. 1b.35.).

In regards to claim 16, Hind and Imamura disclose wherein the first and second communication addresses are uniform resource locator (Hind discloses a client/server relationship in which the client may communicate over an IP network, such as the internet in col. 8 line 65—col. 9 line 20, among the network options. Such a setup requires the use of URLs.).

In regards to claim 17, Hind and Imamura disclose determining whether the second program permits another program to access the data associated with the second program (Imamura fig. 10 discloses different read/write enable/disable combinations. The second program may permit complete, partial, or no access to its data.); and in response to determination that the second program fails to permit another program to access the data associated with the second program denying the first program to access the data associated with the second program (fig. 10.s407 discloses denying all permission.).

In regards to claim 18, Hind and Imamura disclose in response to determination that the second program permits another program to access the data associated with the second program the processor configured to permit the first program to access the data associated with the second program based upon the determination that the first and second addresses match (fig. 10.s406 discloses checking the addresses for a match.).

In regards to claim 19, Hind discloses a computer readable media comprising: a memory (fig. 1a. 28 and 30); computer code stored on the memory (computer code must be stored on memory) executable to receive a first program from a first server (Col. 7 line 34 indicates the workstation may be in a client/server relationship. Col. 9 line 37 indicates the described security method may be applied to any message exchange. Downloading a program is a type of message exchange.); the processor configured to store in the memory the first program and a first

communication address of the first server from which the first program is downloaded (Col. 9 line 23 indicates a globally unique device identifier, which may be considered an address, is stored in the memory shown in fig. 1b.35. When information, such as a program download, is exchanged it must be stored in memory, such as that shown in fig. 1a.28.);

wherein the memory is further configure to store a second program and a second address of a second server from which the second program was downloaded and data associated with the second program (Col. 9 line 37 indicates the security method is performed with any and all message exchanges. This implies there are multiple communications between the client and server, any two of which can be program downloads. Every program download will be handled the same way, i.e. the program and address information are stored in memory.). Hind discloses matching the device identifiers to establish the identity of the program originator in col. 9 lines 57-65.

However, Hind is silent to the processor further configured to execute the first program stored in the memory; in response to a request from the first program executed on the processor to access the data associated with the second program, the process further configured to determine whether the first communication address matches the second communication address; and the processor further configured to permit the first program to access the data associated with the second program based upon the determination that the first communication address of the first server matches the second communication address of the second server.

Imamura discloses running a first program in steps 401-403 of figure 10. In step 406 the identifiers are checked to determine if the first and second addresses match. Steps 407-415

illustrate the different read/write enable/disable combinations possible depending upon the type of identifier match(es) found by Imamura.

It would have been obvious to one of ordinary skill in the art at the time of the invention to use the security matching taught by Imamura in the authentication method of Hind because doing so helps ensure secrecy and security of data, as disclosed by Imamura in column 1 lines 46-48.

In regards to claim 20, Hind and Imamura disclose determining whether the second program permits another program to access the data associated with the second program (Imamura fig. 10 discloses different read/write enable/disable combinations. The second program may permit complete, partial, or no access to its data.); and in response to determination that the second program fails to permit another program to access the data associated with the second program denying the first program to access the data associated with the second program (fig. 10.s407 discloses denying all permission.).

In regards to claim 21, Hind and Imamura disclose extracting the first and second network addresses from a first and second application descriptive file associated with a first and second program respectively (Hind discloses descriptive files in the form of device certificates in fig. 4.).

In regards to claim 22, Hind and Imamura disclose the terminal of claim 8 further comprising: a user interface in communication with the processor wherein the user interface is configured to receive permission for the first program to access the data associated with the second program (Imamura figs. 6a and b disclose setting security level information. The stored information is used in the future to determine permissions relating to access for the first and

second program. Hind discloses storing device certificates and private keys for future determinations in fig. 4.).

In regards to claim 23, Hind and Imamura disclose the terminal of claim 6 further comprising: the processor further configured to determine whether the second program permits another program to access the data associated with the second program (Imamura fig. 10 discloses different read/write enable/disable combinations. The second program may permit complete, partial, or no access to its data.); and in response to determination that the second program permits another program to access the data associated with the second program the processor configured to permit the first program to access the data associated with the second program based upon the determination that the first and second addresses match (fig. 10.s406 discloses checking the addresses for a match.).

In regards to claim 24, Hind and Imamura disclose the terminal of claim 6 wherein the first and second communication addresses are uniform resource locator (Hind discloses a client/server relationship in which the client may communicate over an IP network, such as the internet in col. 8 line 65—col. 9 line 20, among the network options. Such a setup requires the use of URLs.).

In regards to claim 25, Hind and Imamura disclose the terminal of claim 6 wherein the first program is associated with a first portion of the memory (Inherent; When a program is stored into memory a certain "block" of memory is allocated for its use.); the second program is associated with a second portion of the memory and wherein the data of the second program resides in the second portion (Inherent; When a program is stored into memory a certain "block" of memory is allocated for its use, including storage of data related to the program.); and wherein

the processor is further configured to access the second portion to permit the first program to access the data associated with the second program based upon determination that the first and second addresses match (Hind discloses matching the device identifiers to establish the identity of the program originator in col. 9 lines 57-65. Imamura discloses running a first program in steps 401-403 of figure 10. In step 406 the identifiers are checked to determine if the first and second addresses match. Once the match is established the only way to grant access to the second data is for the processor to access the second portion of memory.).

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KERRI M. ROSE whose telephone number is (571) 272-0542. The examiner can normally be reached on Monday through Thursday, 7:00 am - 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Aung MOE can be reached on (571) 272-7314. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aung S. Moe/
Supervisory Patent Examiner, Art Unit 2416

/Kerri M Rose/
Examiner, Art Unit 2416